OAR TCCR Security Subcommittee Recommendations on Web Server Security

The OAR TCCR Security subcommittee stands behind the recommendations included below. They are based on a publicly available document and represent the common wisdom of the IT security community. The recommendations include a problem statement, scope, and a solution to the general problem of web server vulnerability. OAR should move to implement industry standard best practices. The group has made several clarifications and additions to the standard document, including additional practices and procedures, which are more specific to NOAA's OAR sites. Anne Keane's Web Security document was presented at a recent web shop, and it contains a good view of CGI best practices with a slant towards applications used within OAR; it has also been included for reference.

First and foremost, a need was identified to consolidate web personnel and talent. Within the scope of "pooling resources," this is viewed as preferable and more feasible than hardware consolidation. The problem with hardware consolidation (a.k.a. web farms) for many is that OAR's data sets are distributed on local servers, and there are very large amounts of internal data, which are manipulated and served via the web. The resources involved in replicating these databases reliably and securely are too great to justify server hardware consolidation.

To fulfill the need for consolidated web personnel and talent, the subcommittee proposes that one (1) OAR full-time employee dedicated to security for OAR sites be hired and located in Boulder, with a particular dedication to securing public access web servers and IT services. This person would in effect be an available web "consultant" on lab specific web and security projects. This individual is primarily a web server administrator/programmer. While significant improvement is expected with this FTE, it must be recognized that it is not in the scope, nor possible, for one person to develop an OAR-wide web architecture. The selected person needs to be aware of both IIS and apache web servers, and well as the diverse architectures and operating systems involved. This specialist must have unobstructed access to network and server architecture documentation in order to facilitate consulting.

OAR should also assess the integrity of individual web security plans and architectures. The subcommittee considers this to be part of the cross lab assessment topic, which this subcommittee will address in a separate recommendation.

As an additional requirement to those stated below, all web server admins and webmasters need to be on the NCIRT mailing list. This will allow them to keep abreast of security issues and updates as they are published.

As a point of clarification, at some of OAR's labs, network filtering may be accomplished at the server using a host-based firewall. This is deemed acceptable, but it is highly encouraged that it be externally tested for integrity. In some cases, ssh and perhaps even ftp access may be necessary. However, administrators are encouraged to use rsync over the ssh transport (rather than ftp) for updates and web server synchronization.

As stated above, everything below represents the minimal set of best practices as recognized by this subcommittee.

The following a set of "Best Practices" for an Internet Web server, based on my
Own experience and advisory J-042 from the U.S. Department of Energy
Computer Incident Advisory Capability (CIAC)

PROBLEM: Public web servers continue to be attractive targets for hackers seeking to embarrass organizations or promote a political agenda. Good security practices can protect your site from the risks such compromises create.

PLATFORM: Any UNIX platform or NT system being used as a web server.
DAMAGE: Damage can be anything from a denial-of-service attack, the placement of pornographic material, the posting of political messages, or the deletion of files or the placement of malicious software.

SOLUTION: Follow known best practices and apply software patches as soon as they are announced by your incident response team or your vendor.

BEST PRACTICES IN MANAGING WORLD WIDE WEB SERVER SECURITY:

1.Network filtering:

Place your web server(s) in a DMZ. Set your firewall to drop connections to your web server on all ports but http (port 80) or https (port 443).

2.Host based security:

Remove all unneeded services from your web server, keeping FTP (but only if you need it) and a secure login capability such as secure shell. An unneeded service can become an avenue of attack.

Limit the number of persons having administrator or root level access.

Apply relevant security patches as soon as they are announced and tested on a pre-production system. Disallow all remote administration unless it is done using a one-time password or an encrypted link.

If the machine must be administered remotely, require that a secure capability such as secure shell is used to make a secure connection. Do not allow telnet or non-anonymous ftp (those requiring a username and password) connections to this machine from any untrusted site. It would also be good to limit these connections only to a minimum number of secure machines and have those machines reside within your Intranet.

3.Configuring the Web service/application:

If you must use a GUI interface at the console, remove the commands that automatically start the window manager from the .RC startup directories and then create a startup command for the window manager. You can then use the window manager when you need to work on the system, but shut it down when you are done. Do not leave the window manager running for any extended length of time.

Run the web server in a chroot-ed part of the directory tree so it cannot access the real system files.

Run the anonymous FTP server (if you need it) in a chroot-ed part of the directory tree that is different from the web server's tree.

Remove ALL unnecessary files such as phf from the scripts directory /cgi-bin.

Remove the "default" document trees that are shipped with Web servers such as IIS and ExAir.

Apply relevant security patches as soon as they are announced and tested on a pre-production system.

4.Auditing/logging:

Log all user activity and maintain those logs either in an encrypted form on the web server or store them on a separate machine on your Intranet, or write to "write-once" media.

Monitor system logs regularly for any suspicious activity.

Install some trap macros to watch for attacks on the server (such as the PHF attack).

Create macros that run every hour or so that would check the integrity of passwd and other critical files.

When the macros detect a change, they should send an e-mail to the system manager, write a message to logs, set off a pager, etc..

5.Content management:

Do all updates from your Intranet. Maintain your web page originals on a server on your Intranet and make all changes and updates here; then "push" these updates to the public server through an SSH or SSL connection. If you do this on a hourly basis, you can avoid having a corrupted server exposed for a long period of time.

Write a script to download HTML pages and check against a template, if changes are noted, upload the correct version.

6.Intrusion Detection:

Scan your web server periodically with tools like ISS, nmap or Satan to look for vulnerabilities.

Have intrusion detection software monitor the connections to the server. Set the detector to alarm on known exploits and suspicious activities and to capture these sessions for review. This information can help you recover from an intrusion and strengthen your defenses.

BULLETINS PUBLISHED RELATING TO WEB SERVERS:

UNIX Systems

F-11: Unix NCSA httpd Vulnerability http://www.ciac.org/ciac/bulletins/f-11.shtml
H-01: Vulnerabilities in bash http://www.ciac.org/ciac/bulletins/h-01.shtml
I-024: CGI Security Hole in EWS1.1 Vulnerability http://www.ciac.org/ciac/bulletins/i-024.shtml
I-082: HP-UX Netscape Servers Vulnerability http://www.ciac.org/ciac/bulletins/i-082.shtml
I-040: SGI Netscape Navigator Vulnerabilities http://www.ciac.org/ciac/bulletins/i-040.shtml

Domino 4.6 may allow unauthorized writes to remote server drives and server configuration files.
http://www.l0pht.com/advisories/domino2.txt

Excite 1.1 may set encrypted password files world writable. BUGTRAQ Mail Archives: "Security bugs in Excite for Web Servers 1.1" at http://www.netspace.org/cgi-bin/wa?A2=ind9811e&L=bugtraq&F=&S=&P=519

ColdFusion Application Server and unauthorized access to web server data.
http://www.excite.com/computers_and_internet/tech_news/zdnet/?article=/news/19990429/1014542.inp

Windows Systems

I-024: CGI Security Hole in EWS1.1 Vulnerability http://www.ciac.org/ciac/bulletins/i-024.shtml
I-025A: Windows NT based Web Servers File Access Vulnerability http://www.ciac.org/ciac/bulletins/i-025a.shtml

Microsoft bulletins can be found under the Microsoft Security Advisor web page at
http://www.microsoft.com/security/default.asp The following bulletins appeared in "Current Security Bulletins" and "Security Bulletin Archives":
MS99-013: Solution Available for File Viewers Vulnerability. (May 7, 1999)
MS99-012: MSHTML Update Available for Internet Explorer. (April 21, 1999)
MS99-011: Patch Available for "DHTML Edit" Vulnerability. (April 21, 1999)
MS98-019: Patch Available for IIS "GET" Vulnerability. (December 21, 1998)
MS98-016: Update available for "Dotless IP Address" Issue in Microsoft Internet Explorer 4. (October 23, 1998)
MS98-011: Update Available for "Window.External" JScript Vulnerability in Microsoft Internet Explorer 4.0. (August 17, 1998)
MS98-004: Unauthorized ODBC Data Access with Remote Data Services and Internet Information Systems. (July 15, 1998)

"ISAPI Extension vulnerability allows to execute code as SYSTEM" at:
http://www.ntbugtraq.com/page_archives_wa.asp?A2=ind9903&L= ntbugtraq&F=P&S=&P=2439

Internet Explorer 5.0 cached passwords can be reused by another user.
http://www.zdnet.com/zdnn/stories/news/0,4586,1014586,00.html
http://www.zdnet.com/anchordesk/story/story_3351.html

Internet Explorer (3.01, 3.02, 4.0, 4.01) may allow frame spoofing to trick the user Microsoft Knowledgebase Article ID: Q167614: "Update Available For "Frame Spoof" Security Issue"
http://support.microsoft.com/support/kb/articles/q167/6/14.asp

Systems running NCSA HTTPD and Apache HTTPD

G-17: Vulnerabilities in Sample HTTPD CGIs http://ciac.llnl.gov/ciac/bulletins/g-17.shtml
G-20: Vulnerability in NCSA and Apache httpd Servers http://www.ciac.org/ciac/bulletins/g-20.shtml

Apache denial-of-service attack -- Apache httpd (1.2.x, 1.3b3)
http://www.netspace.org/cgi-bin/wa?A1=ind9712e&L=bugtraq#2
http://www.apache.org/dist/patches/apply_to_1.2.4/

no2slash-loop-fix.patch http://www.apache.org/dist/patches/apply_to_1.3b3/
no2slash-loop-fix.patch "HTTP REQUEST_METHOD flaw"
http://www.netspace.org/cgi-bin/wa?A2=ind9901a&L=bugtraq&F=&S=&P=8530

Systems running Netscape Navigator

H-76: Netscape Navigator Security Vulnerability http://www.ciac.org/ciac/bulletins/h-76.shtml
I-082: HP-UX Netscape Servers Vulnerability http://www.ciac.org/ciac/bulletins/i-082.shtml
I-040: SGI Netscape Navigator Vulnerabilities http://www.ciac.org/ciac/bulletins/i-040.shtml

"Reading local files with Netscape Communicator 4.5" at
http://www.geocities.com/ResearchTriangle/1711/b6.html

Netscape Navigator may allow frame spoofing to trick the user Netscape Security Update: "The Frame-Spoofing Vulnerability" http://home.netscape.com/products/security/resources/bugs/framespoofing.html

System running cgi-bin routines

I-013: Count.cgi Buffer Overrun Vulnerability http://www.ciac.org/ciac/bulletins/i-013.shtml
I-014: Vulnerability in GlimpseHTTP and WebGlimpse cgi-bin Packages
http://www.ciac.org/ciac/bulletins/i-014.shtml

IRIX webdist.cgi, handler and wrap programs ftp://sgigate.sgi.com/security/19970501-02-PX
ftp://info.cert.org/pub/cert_advisories/CA-97.12.webdist

"Nlog 1.1b released - security holes fixed"
http://www.netspace.org/cgi-bin/wa?A2=ind9812d&L=bugtraq&F=&S=&P=10302
http://owned.comotion.org/~spinux/index.html

Other useful documents

CIAC also published a document called Securing Internet Information Servers, which has a chapter on Securing World Wide Web Servers http://www.ciac.org/ciac/documents/ciac2308.html

The first is a publication that was developed by SANS and The Intranet Institute after the web server at the U.S. Department of Justice was hacked--"Twelve Mistakes To Avoid In Managing Security-For the Web."
http://www.computerworld.com/home/online9697.nsf/all/971001secure.
SANS also publishes a document called "14 Steps to Avoiding Disaster with Your Web Site."

Another web site that you should book mark is http://www.w3.org/Security/faq/. This is a web security FAQ (Frequently Asked Questions) that is maintained by The World Wide Web Consortium http://www.w3.org/. They have security sections for each of the major operating systems used today for web servers: http://www.w3.org/Security/faq/wwwsf8.html. http://webcompare.internet.com compares how well different web servers compare to the standards.

IF YOUR WEB SITE HAS BEEN HACKED

CIAC recommends the following as you check your web servers:

1. Apply ALL security-related patches for the web server software as well as for the underlying Operating System.
2. Remove ALL unnecessary files such as phf from the scripts directory /cgi-bin. Remove the "default" document trees that are shipped with Web servers such as IIS and ExAir.
3. Validate ALL user accounts on the web server and ensure that they have strong passwords.
4. Validate ALL services and open ports on the web server to ensure there are no Trojanned services.
5. Look for suspicious files in the /dev, /etc, and /tmp directories.

CIAC, the Computer Incident Advisory Capability, is the computer security incident response team for the U.S. Department of Energy (DOE) and the emergency backup response team for the National Institutes of Health (NIH). CIAC is located at the Lawrence Livermore National Laboratory in Livermore, California. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Previous CIAC notices, anti-virus software, and other information are available from the CIAC Computer Security Archive. World Wide Web: http://www.ciac.org/ (or http://ciac.llnl.gov) Anonymous FTP: ftp.ciac.org (or ciac.llnl.gov) Modem access: +1 (925) 423-4753 (28.8K baud) +1 (925) 423-3331 (28.8K baud)

Other references

Microsoft IIS 5.0: "Secure Internet Information Services 5 Checklist" includes a few tweaks to the underlying Windows 2000 OS. www.ntsecurity.net/go/2c.asp?f=/news.asp?IDF=178&TB=news